INFORMATION AND COMPUTATION 116, 162–173 (1995)

Communication Complexity of Sum-Type Functions Invariant under Translation

ULRICH TAMM

Fakultät Mathematik, Universität Bielefeld, Postfach 10 01 31, 33501 Bielefeld, Germany

The communication complexity of a function f denotes the number of bits that two processors have to exchange in order to compute $f(x, y)$, when each processor knows one of the variables x and y, respectively. In this paper the deterministic communication complexity of sum-type functions, such as the Hamming distance and the Lee distance, is examined. Here $f: X \times X \to G$, where X is a finite set and G is an Abelian group, and the sum-type function $f_n: X^n \times X^n \to G$ is defined by $f_n((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sum_{i=1}^{n} f(x_i, y_i)$. Since the functions examined are also translation-invariant, their function matrices are simultaneously diagonalizable and the corresponding eigenvalues can be calculated. This allows to apply a rank lower bound for the communication complexity. The best results are obtained for $G = \mathbb{Z}/2\mathbb{Z}$. For prime numbers $|X|$ in this case the communication complexity of all non-trivial sum-type functions is determined exactly. Exact results are also obtained for the parity of the Hamming distance and the parity of the Lee distance. For the Hamming distance and the Lee distance exact results are only obtained for special parameters n and $|X|$.

1. INTRODUCTION

The notion of communication complexity was first introduced by Yao (1979). Two processors, P_1 and P_2 say, have to determine a function value $f(x, y)$, where $f: X \times Y \to Z$ with finite sets X, Y, and Z. P_1 initially only knows $x \in X$, P_2 only knows $y \in Y$. So according to some protocol P the two processors have to exchange some bits of information, such that finally both know the result $f(x, y)$. Let $L(P)$ denote the maximum number of bits (taken over all possible inputs (x, y)) that must be transmitted, when the protocol P is used. The *communication complexity* $C_2(f)$ then denotes the minimum protocol length, thus $C_2(f) := \min\{L(P) \mid P \text{ computes } f\}$.

It is assumed that the data are transmitted over a binary, noiseless channel. Furthermore, only deterministic protocols are considered. A survey of further concepts and results on communication complexity is given by Orlitsky and El Gamal (1988), Halstenberg (1986), and Lovasz (1990).

An upper bound on $C_2(f)$ results from the following trivial protocol: P_1 sends all the bits of its input x, so that P_2 is able to compute the function value and in turn transmits the result. Hence (w.l.o.g. $|X| \leqslant |Y|$),

$$C_2(f) \leqslant \lceil \log_2(|X|) \rceil + \lceil \log_2(|Z|) \rceil. \tag{1.1}$$

Yao derived a lower bound too: A set $S \times T$ with $S \subset X$, $T \subset Y$ is called a *monochromatic rectangle*, if f is constant on $S \times T$. The *function matrix* $F := (f(x, y))_{x \in X, y \in Y}$ can now be partitioned into monochromatic rectangles. The minimum number of rectangles in such a partition is denoted by $d(f)$ and

$$C_2(f) \geqslant \lceil \log_2 d(f) \rceil. \tag{1.2}$$

In general it is very hard to determine the number $d(f)$, but from (1.2) further lower bounds can be derived. So let $M(f)$ denote the size of the largest monochromatic rectangle in the function matrix F. Then obviously $d(f) \geqslant |X| \cdot |Y| / M(f)$ and

$$C_2(f) \geqslant \left\lceil \log_2 \left(\frac{|X| \cdot |Y|}{M(f)} \right) \right\rceil. \tag{1.3}$$

With each $k \in Z$ is associated the *function-value matrix* $F^{(k)} := (a_{xy})_{x \in X, y \in Y}$, where

$$a_{xy} = \begin{cases} 1, & f(x, y) = k \\ 0, & \text{else.} \end{cases}$$

Mehlhorn and Schmidt (1982) have shown that for Boolean functions $C_2(f_n) \geqslant \log_2(\operatorname{rank}(F))$. This result can easily be extended to

$$C_2(f) \geqslant \left\lceil \log_2 \left(\sum_{k \in Z} \operatorname{rank}(F^{(k)}) \right) \right\rceil. \tag{1.4}$$

Here the rank can be chosen over an arbitrary field; in this paper the rank over the real numbers is used always.

In the Sections 2 and 3 we will examine the communication complexity of *sum-type functions* (following the nota-

0890-5401/95 $6.00

tion of Ahlswede, Cai, and Zhang, 1989). Here additionally a group structure is required for Z. So let $(G, +)$ be an Abelian group. $f_n: X^n \times Y^n \to G$ is called sum-type function, if

$$f_n(x^n, y^n) = \sum_{i=1}^{n} f(x_i, y_i)$$
$$\text{for } x^n := (x_1, \ldots, x_n) \in X^n,\ y^n := (y_1, \ldots, y_n) \in Y^n.$$

A well-known sum-type function is the *Hamming distance* h_n that counts the number of different components in x^n and $y^n \in X^n$. Here $X = Y = \{0, \ldots, q-1\}$, $q \in \mathbb{N}$, and $h: X \times X \to \mathbb{Z}$ is defined by

$$h(x, y) := \begin{cases} 0, & x = y \\ 1, & x \neq y. \end{cases}$$

El Gamal and Pang (1986) determined the communication complexity of the Hamming distance for alphabet size $|X| = q = 2$ up to one bit using lower bound (1.3). They showed that for all $n \in \mathbb{N}$,

$$n + \lceil \log_2(n+1) \rceil - 1 \leqslant C_2(h_n) \leqslant n + \lceil \log_2(n+1) \rceil.$$

The upper bound follows from (1.1), since h_n only takes values in $\{0, \ldots, n\}$.

Ahlswede (1989) extended this result to the alphabet sizes $q = 4, 5$, so for $q = 2, 4, 5$ and $n \in \mathbb{N}$ it holds:

$$|C_2(h_n) - \lceil n \cdot \log_2(q) \rceil - \lceil \log_2(n+1) \rceil| \leqslant 1. \quad (1.5)$$

He also examined the parity of the Hamming distance p_n that is of sum-type too.

Compared to the Hamming distance only the range $\mathbb{Z}$ is replaced by $\mathbb{Z}/2\mathbb{Z}$; thus $p_n: X^n \times X^n \to \mathbb{Z}/2\mathbb{Z}$ with $p(x, y) = h(x, y)$ for $x, y \in X = \{0, \ldots, q-1\}$. $C_2(p_n) = 2$ for $q = 2$ and for all $n \in \mathbb{N}$. For $q = 4$ Ahlswede (1989) obtained

$$C_2(p_n) = n \cdot \log_2(q) + 1 \qquad \text{for all} \quad n \in \mathbb{N}. \quad (1.6)$$

He conjectured that (1.6) is valid for all $q \geqslant 3$.

Further sum-type functions are the set-intersection function (or inner product) m_n, with $m_n: \{0, 1\}^n \times \{0, 1\}^n \to \mathbb{Z}$ and $m(x, y) = x \cdot y$ for $x, y \in \{0, 1\}$, and the Lee distance l_n with

$$l(x, y) := \max\{|x-y|, q - |x-y|\},\ q := |X| = |Y|).$$

The Hamming distance, the parity of the Hamming distance, and the Lee distance have an additional property. These functions are invariant under translation. So $f_n(x^n + z^n, y^n + z^n) = f_n(x^n, y^n)$ for all x^n, y^n and $z^n \in X^n$, where $X = Y = \{0, \ldots, q-1\}$. Sum-type functions that are invariant under translation are examined in this paper. Lower bounds for the communication complexity are obtained using (1.4).

The function matrix F^n of a sum-type function f_n can recursively be described as

$$F^n = \begin{pmatrix} F^{n-1} + a_{11} \cdot J & \cdots & F^{n-1} + a_{1t} \cdot J \\ \vdots & \ddots & \vdots \\ F^{n-1} + a_{s1} \cdot J & \cdots & F^{n-1} + a_{st} \cdot J \end{pmatrix}, \quad (1.7)$$

where $s := |X|$, $t := |Y|$, $J := (1)_{x^{n-1} \in X^{n-1}, y^{n-1} \in Y^{n-1}}$, and

$$F^1 = \begin{pmatrix} a_{11} & \cdots & a_{1t} \\ \vdots & \ddots & \vdots \\ a_{s1} & \cdots & a_{st} \end{pmatrix},$$

is the function matrix of f.

The function-value matrices $F^{n,k}$, $k \in G$, thus have the following recursive structure:

$$F^{n,k} = \begin{pmatrix} F^{n-1, k-a_{11}} & \cdots & F^{n-1, k-a_{1t}} \\ \vdots & \ddots & \vdots \\ F^{n-1, k-a_{s1}} & \cdots & F^{n-1, k-a_{st}} \end{pmatrix}, \quad (1.8)$$

It is well known that the function-value matrices of a function invariant under translation are simultaneously diagonalizable. This fact and recursion (1.8) are exploited to derive some formulae for the eigenvalues of the matrices $F^{n,k}$ in Theorem 2.1.

The best results in this context are obtained for sum-type functions $f_n: X^n \times X^n \to \mathbb{Z}/2\mathbb{Z}$ that are invariant under translation. In this case a product formula for the eigenvalues of the function-value matrices $F^{n,k}$ is derived in which the eigenvalues of the matrices $F^{1,k}$ are the factors. These eigenvalues can easily be computed as a sum of the roots of unity. So in Section 3 the communication complexity of some functions is exactly determined, e.g. (Theorem 3.2),

$$C_2(f_n) = n \cdot \log_2(q) + 1 \quad \text{for every non-constant sum-type function } f_n: X^n \times X^n \to \mathbb{Z}/2\mathbb{Z} \text{ that is invariant under translation, if } q \text{ is a prime number.} \quad (1.9)$$

So here the trivial protocol is optimal.

In Theorem 3.3 Ahlswede's conjecture is proved; hence, for the parity of the Hamming distance (1.6) is valid for all $q \geqslant 3$.

The communication complexity of the parity of the Lee distance $r_n := l_n \pmod 2$ is

$$C_2(r_n) = \begin{cases} n \cdot \log_2(q) + 1, & \text{if } q \text{ is odd} \\ 2, & \text{if } q \text{ is even.} \end{cases} \quad (1.10)$$

If q is even, then $r(x, y) = (x + y) \pmod 2$; thus $r_n(x^n, y^n) = (\sum_{i=1}^n (x_i + y_i)) \pmod 2 = \sum_{i=1}^n x_i \pmod 2 + \sum_{i=1}^n y_i \pmod 2$. So P_1 only has to send the parity of the sum of his components. P_2 then knows the correct value. In Theorem 3.4 Eq. (1.10) is proved for odd q.

These results also have an effect on the asymptotic behaviour of the communication complexity of functions $f_n: X^n \times X^n \to \mathbb{Z}$ that are invariant under translation, since in this case $f_n \pmod 2$ also is invariant under translation and $f_n \pmod 2$ has the range $\mathbb{Z}/2\mathbb{Z}$. But it is not possible to exchange fewer bits for the computation of f_n than for the computation of $f_n \pmod 2$. Thus, e.g., for any such function with prime $q := |X|$ we have $\lim_{n \to \infty} (1/n) \cdot C_2(f_n) = \log_2(q)$ (the upper bound obtained with (1.1) has the same order of magnitude).

The function value matrices $H^{n,k}$ of the Hamming distance are well known in algebraic coding theory as the Hamming association scheme. Their eigenvalues are the *Krawtchouk polynomials*,

$$K_k(x, n) := \sum_{j=0}^{k} (-1)^j \cdot (q-1)^{k-j} \cdot \binom{x}{j} \cdot \binom{n-x}{k-j},$$
$$n \in \mathbb{N}, \quad k \in \{0, ..., n\}, \quad x \in \mathbb{R}, \tag{1.11}$$

evaluated for the integer numbers $x := 0, ..., n$ (see, e.g., MacWilliams and Sloane, 1977, p. 151).

Thus, if for $k = 0, ..., n$ the Krawtchouk polynomials $K_k(x, n)$ have no integral zeros, then all the eigenvalues of the function-value matrices $H^{n,k}$ are different from 0 and each of those matrices has full rank q^n. In this case bound (1.4) yields $C_2(h_n) \geq \lceil n \cdot \log_2(q) + \log_2(n+1) \rceil$, so that (1.5) holds. In Theorem 4.1 it is shown that (1.5) is valid for $n = p^t - 1$ ($t \in \mathbb{N}$), where p is a prime divisor of q.

There are several results concerning the integral zeros of the Krawtchouk polynomials motivated by the theory of perfect codes (e.g., van Lint, 1975) and the inversion of the Radon-transform (Diaconis and Graham, 1985). It turns out that in general it is very hard to determine, if there exist integral zeros. But theoretical and numerical analyses of Chihara und Stanton (1990) give rise to the conjecture that there are only a very few integral zeros, such that (1.5) is valid in general. For alphabet size $q = 2$, Spieker (1992) recently gave a new proof for Eq. (1.5) (and all $n \in \mathbb{N}$), hereby showing that there are not too many integral zeros of the Krawtchouk polynomials in this special case.

The last functions that are invariant under translation treated in this paper are the Hamming distance (modulo 3), denoted by d_n, and the Lee distance.

With number theoretical methods it can be shown that for certain $n \in \mathbb{N}$ all the eigenvalues of the function-value matrices are different from 0. So (Theorem 5.1)

$$C_2(d_n) \geq \begin{cases} \lceil \log_2(3) + n \cdot \log_2(q) \rceil, & n \text{ even} \\ \lceil \log_2(3 \cdot q^n - (q-1)^n) \rceil, & n \text{ odd.} \end{cases} \tag{1.12}$$

For the Lee distance l_n Theorem 6.1 only gives a result in the following special case:

$$\left| C_2(l_n) - \lceil n \cdot \log_2(q) \rceil - \left\lceil \log_2\left(\frac{q-1}{2} \cdot n + 1\right) \right\rceil \right| \leq 1,$$

for a prime number q and

$$n = \delta \cdot q^t + 2 \cdot q^{t-1} + \cdots + 2 \cdot q + 2,$$
$$\delta \in \{1, 2\}, \quad t \in \mathbb{N}. \tag{1.13}$$

2. SUM-TYPE FUNCTIONS INVARIANT UNDER TRANSLATION

From now on let $X := \{0, ..., q-1\}$, $q \in \mathbb{N}$, let $(G, +)$ be an Abelian group, and let $f_n: X^n \times X^n \to G$ be a sum-type function that is invariant under translation. Hence,

$$f_n(x^n + z^n, y^n + z^n) = f_n(x^n, y^n)$$
$$\text{for all} \quad n \in \mathbb{N}, \quad x^n, y^n, z^n \in X^n.$$

The most important examples of such functions are the Hamming distance and the Lee distance, which have intensively been studied in coding theory.

We have to introduce some further notations for the following disussion. For $x^n \in X^n$ let the *weight* $w(x^n)$ and the *composition* $c(x^n)$ be defined as:

$$w(x^n) := f_n(0^n, x^n), \qquad \text{where} \quad 0^n := (0, 0, ..., 0), \tag{2.1}$$

$$c(x^n) = (a_0, a_1, ..., a_{q-1}), \qquad \text{with} \quad a_i := |\{j: x_j = i\}|. \tag{2.2}$$

As usual, let $A \otimes B$ denote the *Kronecker product* of the matrices A and B. $A^{\otimes n}$ is the n-fold Kronecker product of the matrix A. By F_q we denote the *Fourier matrix* $(\omega^{i \cdot j})_{i,j=0,...,q-1}$, where ω is a primitive qth root of unity. Finally we shall write

$$Z_q = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{2.3}$$

for the matrix representation of the generator of the cyclic group of order q. Equation (1.6) implies that the function

matrix $F^n := (f_n(x^n, y^n))_{x^n, y^n \in X^n}$ has recursive structure (here $w(t) := f(0, t)$ for $t = 0, \ldots, q-1$, $J := (1)_{x^{n-1}, y^{n-1} \in X^{n-1}}$)

$$F^n = \begin{pmatrix} F^{n-1} + w(0) \cdot J & F^{n-1} + w(1) \cdot J & \cdots & F^{n-1} + w(q-1) \cdot J \\ F^{n-1} + w(q-1) \cdot J & F^{n-1} + w(0) \cdot J & \cdots & F^{n-1} + w(q-2) \cdot J \\ \vdots & \vdots & \ddots & \vdots \\ F^{n-1} + w(1) \cdot J & F^{n-1} + w(2) \cdot J & \cdots & F^{n-1} + w(0) \cdot J \end{pmatrix} \tag{2.4}$$

with

$$F^1 = \begin{pmatrix} w(0) & w(1) & \cdots & w(q-1) \\ w(q-1) & w(0) & \cdots & w(q-2) \\ \vdots & \vdots & \ddots & \vdots \\ w(1) & w(2) & \cdots & w(0) \end{pmatrix} = \sum_{t=0}^{q-1} w(t) \cdot Z_q^t.$$

LEMMA 2.1. *For $n \geqslant 1$, $k \in G$, let $F^{n,k}$ be the function-value matrix of a sum-type function invariant under translation. Then*

$$F^{n,k} = \sum_{g \in G} F^{1,g} \otimes F^{n-1,k-g}, \tag{2.5}$$

$$F^{n,k} = \sum_{\substack{t^n \in X^n: \\ w(t^n) = k}} Z_q^{t_1} \otimes Z_q^{t_2} \otimes \cdots \otimes Z_q^{t_n}$$

$$\text{with} \quad t^n = (t_1, t_2, \ldots, t_n) \in X^n. \tag{2.6}$$

Proof. (a) (1.7) and (2.4) imply that for $w(t) = f(0, t)$, $t \in \{0, \ldots, q-1\}$,

$$F^{n,k} = \begin{pmatrix} F^{n-1,k-w(0)} & F^{n-1,k-w(1)} & \cdots & F^{n-1,k-w(q-1)} \\ F^{n-1,k-w(q-1)} & F^{n-1,k-w(0)} & \cdots & F^{n-1,k-w(q-2)} \\ \vdots & \vdots & \ddots & \vdots \\ F^{n-1,k-w(1)} & F^{n-1,k-w(2)} & \cdots & F^{n-1,k-w(0)} \end{pmatrix} \tag{2.7}$$

with

$$F^{1,k} = \sum_{t \in X: w(t) = k} Z_q^t. \tag{2.8}$$

Hence

$$\begin{aligned} F^{n,k} &= \sum_{t=0}^{q-1} Z_q^t \otimes F^{n-1,k-w(t)} \\ &= \sum_{g \in G} \sum_{t \in X: w(t) = g} Z_q^t \otimes F^{n-1,k-g} \\ &= \sum_{g \in G} \left(\sum_{t \in X: w(t) = g} Z_q^t \right) \otimes F^{n-1,k-g} \\ &= \sum_{g \in G} F^{1,g} \otimes F^{n-1,k-g}. \end{aligned} \tag{2.9}$$

(b) (Induction on n).

For $n = 1$, of course, (2.8) results. Assume that (2.6) is proved for all $F^{n-1,k}$, $k \in G$. By (2.9) and the induction hypothesis now

$$\begin{aligned} F^{n,k} &= \sum_{g \in G} \sum_{t_1 \in X: w(t_1) = g} Z_q^{t_1} \\ &\quad \otimes \sum_{\substack{(t_2, t_3, \ldots, t_n) \in X^{n-1}: \\ w(t_2, t_3, \ldots, t_n) = k-g}} Z_q^{t_2} \otimes Z_q^{t_3} \otimes \cdots \otimes Z_q^{t_n} \\ &= \sum_{g \in G} \sum_{t_1 \in X: w(t_1) = g} \\ &\quad \times \sum_{\substack{(t_2, t_3, \ldots, t_n) \in X^{n-1}: \\ w(t_2, t_3, \ldots, t_n) = k-g}} Z_q^{t_1} \otimes Z_q^{t_2} \otimes \cdots \otimes Z_q^{t_n} \\ &= \sum_{\substack{t^n \in X^n: \\ w(t^n) = k}} Z_q^{t_1} \otimes Z_q^{t_2} \otimes \cdots \otimes Z_q^{t_n}. \quad \blacksquare \end{aligned}$$

THEOREM 2.1. *Let $e_{i^n}(k)$, $i^n = (i_1, i_2, \ldots, i_n) \in X^n$, be the eigenvalues of the matrix $F^{n,k}$, $n \geqslant 1$, $k \in G$. The properties*

$$e_{(i_1, i_2, \ldots, i_n)}(k) = \sum_{g \in G} e_{i_1}(g) \cdot e_{(i_2, i_3, \ldots, i_n)}(k-g), \tag{2.10}$$

$$e_{i^n}(k) = \sum_{\substack{t^n \in X^n: \\ w(t^n) = k}} \omega^{\langle i^n, t^n \rangle}, \tag{2.11}$$

hold, where $t^n := (t_1, t_2, \ldots, t_n) \in X^n$, $\langle i^n, t^n \rangle := \sum_{j=1}^n i_j \cdot t_j$ and ω is a primitive qth root of unity,

$$e_{(i_1, i_2, \ldots, i_n)}(k) = \sum_{k_1 + k_2 + \cdots + k_n = k} e_{i_1}(k_1) \cdot e_{i_2}(k_2) \cdot \cdots \cdot e_{i_n}(k_n), \tag{2.12}$$

if $G = \mathbb{Z}$, then $e_{(i_1, i_2, \ldots, i_n)}(k)$ is the coefficient of z^k in the polynomial

$$\sum_{k \in \mathbb{Z}} e_{(i_1, i_2, \ldots, i_n)}(k) \cdot z^k = \prod_{j=1}^n \left(\sum_{g \in \mathbb{Z}} e_{i_j}(g) \cdot z^g \right). \tag{2.13}$$

Proof. (a) It is well known that the function-value matrices $F^{n,k}$ of a sum-type function invariant under translation are simultaneously diagonalized by the matrix $F_q^{\otimes n}$ (cf. Delsarte, 1973, p. 23 or Davis, 1979). So for $n \geqslant 1$, $k \in G$, $(F_q^{\otimes n})^{-1} \cdot F^{n,k} \cdot F_q^{\otimes n} = D^{n,k}$, where $D^{n,k}$ is the diagonal matrix with the eigenvalues of $F^{n,k}$. With the computation rules for the Kronecker product we can conclude that

$$\begin{aligned} D^{n,k} &= (F_q^{\otimes n})^{-1} \cdot F^{n,k} \cdot F_q^{\otimes n} \\ &= (F_q^{\otimes n})^{-1} \cdot \left(\sum_{g \in G} F^{1,g} \otimes F^{n-1,k-g} \right) \cdot F_q^{\otimes n} \qquad \text{(by (2.5))} \\ &= \sum_{g \in G} (F_q^{\otimes n})^{-1} \cdot (F^{1,g} \otimes F^{n-1,k-g}) F_q^{\otimes n} \end{aligned}$$

$$= \sum_{g \in G} (F_q^{-1} \otimes [F_q^{\otimes(n-1)}]^{-1}) \cdot (F^{1,g} \otimes F^{n-1,k-g}) \cdot (F_q \otimes F_q^{\otimes(n-1)})$$

$$= \sum_{g \in G} (F_q^{-1} \cdot F^{1,g} \cdot F_q) \otimes ((F_q^{\otimes(n-1)})^{-1} \cdot F^{n-1,k-g} \cdot F_q^{\otimes(n-1)})$$

$$= \sum_{g \in G} D^{1,g} \otimes D^{n-1,k-g}$$

$$= \sum_{g \in G} \begin{pmatrix} e_0(g) \cdot D^{n-1,k-g} & & & \\ & e_1(g) \cdot D^{n-1,k-g} & & \\ & & \ddots & \\ & & & e_{q-1}(g) \cdot D^{n-1,k-g} \end{pmatrix},$$

and by induction $e_{(i_1, i_2, \ldots, i_n)}(k) = \sum_{g \in G} e_{i_1}(g) \cdot e_{(i_2, i_3, \ldots, i_n)}(k-g)$.

(b) $F^{1,k} = \sum_{t \in X: w(t)=k} Z_q^t$ by definition (2.8). Since the eigenvalues of Z_q^t are $\omega^{i \cdot t}$, $i = 0, \ldots, q-1$, we have for the eigenvalues of $F^{1,k}$: $e_i(k) = \sum_{t \in X: w(t)=k} \omega^{i \cdot t}$, for $i \in \{0, \ldots, q-1\}$.

By (a) and induction now

$$\begin{aligned} & e_{(i_1, i_2, \ldots, i_n)}(k) \\ &= \sum_{g \in G} e_{i_1}(g) \cdot e_{(i_2, i_3, \ldots, i_n)}(k-g) \\ &= \sum_{g \in G} \left(\sum_{t_1 \in X: w(t_1)=g} \omega^{i_1 \cdot t_1} \right) \\ &\quad \cdot \left(\sum_{\substack{(t_2, t_3, \ldots, t_n) \in X^{n-1}: \\ w(t_2, t_3, \ldots, t_n) = k-g}} \omega^{i_2 \cdot t_2 + \cdots + i_n \cdot t_n} \right) \\ &= \sum_{g \in G} \sum_{t_1 \in X: w(t_1)=g} \\ &\quad \times \sum_{\substack{(t_2, t_3, \ldots, t_n) \in X^{n-1}: \\ w(t_2, t_3, \ldots, t_n) = k-g}} \omega^{i_1 \cdot t_1 + i_2 \cdot t_2 + \cdots + i_n \cdot t_n} \\ &= \sum_{\substack{t^n \in X^n: \\ w(t^n)=k}} \omega^{\langle i^n, t^n \rangle}, \end{aligned}$$

(2.12) and (2.13) can easily be derived from (2.10). ∎

Remark. It is clear from (2.12) that, because of the commutativity, the eigenvalue $e_{i^n}(k)$ only depends on the composition $c(i^n)$. So, if i^n and j^n have the same composition $c(i^n) = c(j^n)$, then $e_{i^n}(k) = e_{j^n}(k)$.

3. RANGE $G = \mathbb{Z}/2\mathbb{Z}$

Let $X := \{0, \ldots, q-1\}$ and let $f_n: X^n \times X^n \to \mathbb{Z}/2\mathbb{Z}$ be a sum-type function that is invariant under translation with function-value matrices $F^{n,0}$ and $F^{n,1}$. An eigenvalue $e_{i^n}(k)$, $k \in \{0, 1\}$, only depends on the composition $(a_0, a_1, \ldots, a_{q-1})$ of i^n. So let w.l.o.g.

$$i^n = (\underbrace{0, \ldots, 0}_{a_0}, \underbrace{1, \ldots, 1}_{a_1}, \ldots, \underbrace{q-1, \ldots, q-1}_{a_{q-1}}).$$

Furthermore, let $\sigma := q-1$. For $k, k_1, \ldots, k_n \in \mathbb{Z}/2\mathbb{Z}$ (2.12) implies that

$$\begin{aligned} e_{i^n}(k) &= \sum_{k_1 + k_2 + \cdots + k_n = k} e_{i_1}(k_1) \cdot e_{i_2}(k_2) \cdot \cdots \cdot e_{i_n}(k_n) \\ &= \sum_{k_1 + k_2 + \cdots + k_n = k} e_0(k_1) \cdot \cdots \cdot e_0(k_{a_0}) \cdot e_1(k_{a_0+1}) \cdot \cdots \\ &\quad \cdot e_1(k_{a_0+a_1}) \cdot \cdots \cdot e_\sigma(k_{n-a_\sigma+1}) \cdot \cdots \cdot e_\sigma(k_n). \end{aligned}$$

For $t_j \in \{0, 1\}$ and $j := 0, \ldots, q-1$ we define

$$E_j(t_j) := \sum_{k_{j1} + \cdots + k_{ja_j} = t_j} e_j(k_{j1}) \cdot \cdots \cdot e_j(k_{ja_j}). \tag{3.1}$$

Now let

$$Y := \{y_1, \ldots, y_m\} = \{j \in \{0, \ldots, q-1\} : a_j \neq 0\}, \; m := |Y|. \tag{3.2}$$

So with $t_1, t_2, \ldots, t_m \in \mathbb{Z}/2\mathbb{Z}$,

$$e_{i^n}(k) = \sum_{t_1 + \cdots + t_m = k} \prod_{j=1}^{m} E_{y_j}(t_j). \tag{3.3}$$

Here $e_j(0)$ and $e_j(1)$, $j := 0, \ldots, q-1$, are the eigenvalues of the matrices $F^{1,0}$ and $F^{1,1}$. Now from (2.11) it follows that

$$e_j(0) + e_j(1) = \sum_{t=0}^{q-1} \omega^{jt} = \begin{cases} q, & j = 0 \\ 0, & j = 1, \ldots, \sigma; \end{cases}$$

hence

$$e_0(0) = q - e_0(1), \; e_j(0) = -e_j(1) \quad \text{for} \quad j = 1, \ldots, \sigma. \tag{3.4}$$

Obviously, for $k, k_1, k_2, \ldots, k_n \in \mathbb{Z}/2\mathbb{Z}$,

$$k_1 + k_2 + \cdots + k_n = \begin{cases} 0, & \text{if an even number of the } k_i = 1 \\ 1, & \text{if an odd number of the } k_i = 1. \end{cases} \tag{3.5}$$

THEOREM 3.1. *Let $f_n: X^n \times X^n \to \mathbb{Z}/2\mathbb{Z}$ be a sum-type function invariant under translation and let $e_{i^n}(k)$ be an eigenvalue of the function value matrix $F^{n,k}$, $k \in \{0, 1\}$, of f_n with composition $(a_0, a_1, \ldots, a_{q-1})$ of i^n. Then*

$$e_{i^n}(k) = \begin{cases} \frac{1}{2} \cdot (q^n + (-1)^k \cdot (2 \cdot e_0(0) - q)^n & \text{for } i^n = (0, \ldots, 0) \\ (-1)^k \cdot 2^{n-a_0-1} \cdot (2 \cdot e_0(0) - q)^{a_0} & \\ \quad \cdot \prod_{\substack{j=1 \\ a_j \neq 0}}^{q-1} (e_j(0))^{a_j} & \text{else.} \end{cases} \tag{3.6}$$

Proof. First the numbers $E_j(t_j)$, $j := 0, \ldots, q-1$ and $t_j := 0, 1$ have to be determined. So let $x := e_0(0)$. From (3.4) it follows that $q - x = e_0(1)$. Hence (3.1) yields

$$E_0(t_0) = \sum_{k_{01}+\cdots+k_{0a_0}=t_0} e_0(k_{01}) \cdot \cdots \cdot e_0(k_{0a_0})$$

$$= \begin{cases} x^{a_0} + \binom{a_0}{2} x^{a_0-2}(q-x)^2 \\ \quad + \binom{a_0}{4} x^{a_0-4}(q-x)^4 + \cdots, \quad t_0 = 0, \\ a_0 x^{a_0-1}(q-x) + \binom{a_0}{3} x^{a_0-3}(q-x)^3 \\ \quad + \binom{a_0}{5} x^{a_0-5}(q-x)^5 + \cdots, \quad t_0 = 1, \end{cases}$$

$$= \begin{cases} \frac{1}{2} \cdot [(x+(q-x))^{a_0} + (x-(q-x))^{a_0}], & t_0 = 0, \\ \frac{1}{2} \cdot [(x+(q-x))^{a_0} - (x-(q-x))^{a_0}], & t_0 = 1, \end{cases}$$

$$= \frac{1}{2} \cdot (q^{a_0} + (-1)^{t_0} \cdot (2x-q)^{a_0})$$

$$= \frac{1}{2} \cdot (q^{a_0} + (-1)^{t_0} \cdot (2e_0(0)-q)^{a_0}).$$

Now let $j \in \{1, \ldots, q-1\}$ and $x := e_j(0)$. (3.4) implies that $-x = e_j(1)$, so that

$$E_j(t_j) = \sum_{k_{j1}+\cdots+k_{ja_j}=t_j} e_j(k_{j1}) \cdot \cdots \cdot e_j(k_{ja_j})$$

$$= \sum_{k_{j1}+\cdots+k_{ja_j}=t_j} (-1)^{k_{j1}} x \cdot \cdots \cdot (-1)^{k_{ja_j}} x$$

$$= x^{a_j} \cdot \sum_{k_{j1}+\cdots+k_{ja_j}=t_j} (-1)^{k_{j1}+\cdots+k_{ja_j}}$$

$$= x^{a_j} \cdot (-1)^{t_j} \cdot \sum_{k_{j1}+\cdots+k_{ja_j}=t_j} 1$$

$$= (-1)^{t_j} \cdot x^{a_j} \cdot 2^{a_j-1} = (-1)^{t_j} \cdot 2^{a_j-1} \cdot (e_j(0))^{a_j},$$

because (3.5) implies that for $t_j = 0$ (analogously for $t_j = 1$)

$$\sum_{k_{j1}+\cdots+k_{ja_j}=0} 1 = \binom{a_j}{0} + \binom{a_j}{2} + \binom{a_j}{4} + \cdots = 2^{a_j-1}.$$

Applying (3.3) the following result for the eigenvalues $e_{i^n}(k)$ can be deduced:

Case 1. $a_0 = n$. So $i^n = (0, \ldots, 0)$ and $t_0 = k$:

$$e_{(0,\ldots,0)}(k) = E_0 = \tfrac{1}{2} \cdot (q^n + (-1)^k \cdot (2e_0(0)-q)^n).$$

Case 2. $a_0 = 0$. From (3.2) and (3.3) it follows that

$$e_{i^n}(k) = \sum_{t_1+\cdots+t_m=k} \prod_{j=1}^{m} E_{y_j}(t_j)$$

$$= \sum_{t_1+\cdots+t_m=k} \prod_{j=1}^{m} (-1)^{t_j} \cdot 2^{a_{yj}-1} \cdot (e_{y_j}(0))^{a_{yj}}$$

$$= \prod_{j=1}^{m} (e_{y_j}(0))^{a_{yj}} \cdot \prod_{j=1}^{m} 2^{a_{yj}-1} \cdot \sum_{t_1+\cdots+t_m=k} (-1)^{t_1+\cdots+t_m}$$

$$= \prod_{\substack{j=1 \\ a_j \neq 0}}^{q-1} (e_j(0))^{a_j} \cdot 2^{n-m} \cdot (-1)^k \cdot \sum_{t_1+\cdots+t_m=k} 1$$

$$= (-1)^k \cdot \prod_{\substack{j=1 \\ a_j \neq 0}}^{q-1} (e_j(0))^{a_j} \cdot 2^{n-m} \cdot 2^{m-1}$$

$$= (-1)^k \cdot 2^{n-1} \cdot \prod_{\substack{j=1 \\ a_j \neq 0}}^{q-1} (e_j(0))^{a_j},$$

since by (3.5) $\sum_{t_1+\cdots+t_m=k} 1 = 2^{m-1}$.

Case 3. $1 \leqslant a_0 \leqslant n-1$. Applying (3.2) and (3.3) again yields

$$e_{i^n}(k) = \sum_{t_1+\cdots+t_m=k} \prod_{j=1}^{m} E_{y_j}(t_j)$$

$$= \sum_{t_1+\cdots+t_m=k} \tfrac{1}{2} \cdot [q^{a_0} + (-1)^{t_1}(2e_0(0)-q)^{a_0}] \cdot \prod_{j=2}^{m} (-1)^{t_j} \cdot (e_{y_j}(0))^{a_{yj}} \cdot 2^{a_{yj}-1}$$

$$= \prod_{j=1}^{m} (e_{y_j}(0))^{a_{yj}} \cdot \prod_{j=2}^{m} 2^{a_{yj}-1} \cdot \tfrac{1}{2} \cdot \sum_{t_0+\cdots+t_m=k} [q^{a_0} + (-1)^{t_1}(2e_0(0)-q)^{a_0}] \cdot (-1)^{k-t_1}$$

$$= \prod_{\substack{j=1 \\ a_j \neq 0}}^{q-1} (e_j(0))^{a_j} \cdot 2^{n-a_0-m} \cdot (-1)^k \cdot \sum_{t_1+\cdots+t_m=k} [(-1)^{t_1} q^{a_0} + (2e_0(0)-q)^{a_0}]$$

$$= (-1)^k \cdot \prod_{\substack{j=1 \\ a_j \neq 0}}^{q-1} (e_j(0))^{a_j} \cdot 2^{n-a_0-m} \cdot \left[q^{a_0} \cdot \sum_{t_1+\cdots+t_m=k} (-1)^{t_1} + (2e_0(0)-q)^{a_0} \cdot \sum_{t_1+\cdots+t_m=k} 1 \right]$$

$$= (-1)^k \cdot \prod_{\substack{j=1 \\ a_j \neq 0}}^{q-1} (e_j(0))^{a_j} \cdot 2^{n-a_0-m} \cdot 2^{m-1} \cdot (2e_0(0)-q)^{a_0}$$

$$= (-1)^k \cdot 2^{n-a_0-1} \cdot \prod_{\substack{j=1 \\ a_j \neq 0}}^{q-1} (e_j(0))^{a_j} \cdot (2e_0(0)-q)^{a_0}$$

since $\sum_{t_1+\cdots+t_m=k} 1 = 2^{m-1}$ and $\sum_{t_1+\cdots+t_m=k} (-1)^{t_1} = \sum_{t_1=0}^{1} (-1)^{t_1} \sum_{t_2+\cdots+t_m=k} 1 = 2^{m-2} - 2^{m-2} = 0$. ∎

Now, from (3.6) we know that all the eigenvalues of $F^{n,k}$, $k \in \{0, 1\}$, are different from 0, if the eigenvalues $e_j(0)$, $j = 1, ..., q-1$, of $F^{1,0}$ differ from 0 and if $e_0(0) \neq q/2$. With this knowledge we now will exactly determine the communication complexity of some functions.

THEOREM 3.2. *Let $f_n: \{0, ..., q-1\}^n \times \{0, ..., q-1\}^n \to \mathbb{Z}/2\mathbb{Z}$ be a non-constant sum-type function that is invariant under translation, and let q be an odd prime number. Then for all $n \in \mathbb{N}$*

$$C_2(f_n) = \lceil n \cdot \log_2(q) \rceil + 1.$$

Proof. Let $F^{1,0} = Z_q^{s_1} + Z_q^{s_2} + \cdots + Z_q^{s_t}$, $s_1, ..., s_t \in \{0, ..., q-1\}$. So (2.11) implies that $e_0(0) = \sum_{r=0}^{t} \omega^{0 \cdot s_r} = t \in \mathbb{N}$; hence $e_0(0) \neq q/2$, since q is odd. Moreover, $\{s_1, ..., s_t\} \neq \{0, ..., q-1\}$, as f is non-constant. So $e_j(0) = \sum_{r=0}^{t} \omega^{j \cdot s_r} \neq 1 + \omega + \cdots + \omega^{q-1}$. But, since q is prime, $1 + \omega + \cdots + \omega^{q-1} = 0$ is the only possible representation of 0 as a sum of roots of unity. Thus we can conclude that $e_j(0) \neq 0$ for $j = 1, ..., q-1$. So with (3.6) it is easy to see that the function-value matrices $F^{n,0}$ and $F^{n,1}$ have full rank q^n for all $n \in \mathbb{N}$, and the lower bound (1.4) implies that

$$C_2(f_n) \geq \lceil \log_2(\operatorname{rank}(F^{n,0}) + \operatorname{rank}(F^{n,1})) \rceil$$
$$= \lceil \log_2(2 \cdot q^n) \rceil = \lceil n \cdot \log_2(q) + 1 \rceil.$$

Using the upper bound (1.1) we can conclude that $C_2(f_n) = \lceil n \cdot \log_2(q) \rceil + 1$. ∎

COROLLARY 3.1. *Let $f_n: \{0, ..., q-1\}^n \times \{0, ..., q-1\}^n \to \mathbb{Z}$ be a non-constant sum-type function invariant under translation, and let q be an odd prime number. Then* $\lim_{n \to \infty} (1/n) \cdot C_2(f_n) = \log_2(q)$.

Proof. If all the function values $f(x, y)$, $x, y \in \{0, ..., q-1\}$, have the same parity, then we will consider the function f', defined by $f'(x, y) := f(x, y) - M$, where $M := \min_{x,y}\{f(x, y)\}$. Then $f'_n((x_1, ..., x_n), (y_1, ..., y_n)) = \sum_{i=1}^{n} f'(x_i, y_i) = \sum_{i=1}^{n} f(x_i, y_i) - n \cdot M$, so that for the function-value matrix $F'^{n,k}$, $F'^{n,k} = F^{n,k+nM}$ holds. Now f' only takes even values. We can once more transform f' to an equivalent function f'' by dividing all the function values by $\gcd(f'(x, y))_{x,y \in \{0, ..., q-1\}}$. As f is non-constant, f'' must take even values as well as odd values.

The two processors can separately execute these transformations; hence the communication complexity is not influenced. So w.l.o.g. we can assume that f takes even values as well as odd values. Then the function $f_n \pmod 2$ is non-constant too. This function is also invariant under translation and takes values in $\mathbb{Z}/2\mathbb{Z}$; hence by Theorem 3.2, $C_2(f_n \pmod 2) = \lceil n \cdot \log_2(q) \rceil + 1$.

However, then $C_2(f_n) \geq \lceil n \cdot \log_2(q) \rceil$, because otherwise the two processors could first compute f_n and thereafter send the parity bit. So it remains to show that the upper bound obtained by the trivial protocol is of the same order of magnitude. $f: \{0, ..., q-1\} \times \{0, ..., q-1\} \to \mathbb{Z}$ can take at most q different values. Now $f_n((x_1, ..., x_n), (y_1, ..., y_n)) = \sum_{i=1}^{n} f(x_i, y_i)$ is a sum of n function values.

Because of the commutativity the order of the summands is not of importance. Hence f_n can take at most $\binom{n+q-1}{q}$ different values, and (1.1) yields

$$C_2(f_n) \leq \lceil n \cdot \log_2(q) \rceil + \left\lceil \log_2 \binom{n+q-1}{q} \right\rceil$$
$$\leq \lceil n \cdot \log_2(q) \rceil + \lceil \log_2(n+q-1)^q \rceil.$$

So $\lceil n \cdot \log_2(q) \rceil \leq C_2(f_n) \leq \lceil n \cdot \log_2(q) \rceil + \lceil q \cdot \log_2(n+q-1) \rceil$ and, hence, $\lim_{n \to \infty} (1/n) \cdot C_2(f_n) = \log_2(q)$. ∎

Remark. The proof of Theorem 3.2 shows that $C_2(f_n) = \lceil n \cdot \log_2(q) \rceil + 1$ does not depend on the property that $q = |X|$ is a prime number. It is only requested that for the set $\{s_1, ..., s_t: F^{1,0} = Z_q^{s_1} + \cdots + Z_q^{s_t}\}$ the following conditions hold:

(i) $t \neq q/2$,

(ii) $\{s_1, ..., s_t\} \neq \{j \cdot m: j = 0, ..., q/m - 1\}$ for a divisor m of q.

THEOREM 3.3. *Let $p_n = h_n \pmod 2$ denote the parity of the Hamming distance. For alphabet size $q \geq 3$ then $C_2(p_n) = \lceil n \cdot \log_2(q) \rceil + 1$.*

Proof. $P^{1,0} = Z_q^0$, the identity matrix, and $P^{1,1} = Z_q^1 + \cdots + Z_q^{q-1}$. So (2.11) yields

$$e_0(0) = e_1(0) = \cdots = e_{q-1}(0) = 1,$$
$$e_0(1) = \omega^{0 \cdot 1} + \omega^{0 \cdot 2} + \cdots + \omega^{0 \cdot (q-1)} = q - 1,$$
$$e_j(1) = \omega^{j \cdot 1} + \omega^{j \cdot 2} + \cdots + \omega^{j \cdot (q-1)}$$
$$= -1 \quad \text{for} \quad j = 1, ..., q-1.$$

Now let i^n have Hamming weight $n - a_0$ (a_0 zeros). Then

$$e_{i^n}(k) = \begin{cases} \frac{1}{2} \cdot (q^n + (-1)^k (2-q)^n) & \text{for } i^n = (0, ..., 0) \\ (-1)^k \cdot 2^{n-a_0-1} \cdot (2-q)^{a_0} & \text{else.} \end{cases}$$

So for $q \geq 3$ all the eigenvalues of $F^{n,0}$ and $F^{n,1}$ are different from 0. Hence both matrices have full rank q^n, so that

applying the bounds (1.1) and (1.4) we now can conclude that $C_2(p_n) = \lceil n \cdot \log_2(q) \rceil + 1$. ∎

THEOREM 3.4. *Let $r_n := l_n \pmod 2$ denote the parity of the Lee distance and let the alphabet size q be an odd number. Then $C_2(r_n) = \lceil n \cdot \log_2(q) \rceil + 1$.*

Proof. The function-value matrix $R^{1,0}$ is given (see also Section 6) by

$$R^{1,0} = \begin{cases} Z_q^0 + Z_q^2 + Z_q^4 + \cdots + Z_q^{(q-1)/2} + Z_q^{(q+1)/2} + \cdots \\ \qquad + Z_q^{q-4} + Z_q^{q-2}, & q \equiv 1 \pmod 4 \\ Z_q^0 + Z_q^2 + Z_q^4 + \cdots + Z_q^{(q-3)/2} + Z_q^{(q+3)/2} + \cdots \\ \qquad + Z_q^{q-4} + Z_q^{q-2}, & q \equiv -1 \pmod 4. \end{cases}$$

As q is odd and $e_0(0) \in \mathbb{N}$, we have $e_0(0) \neq q/2$. For the eigenvalues $e_j(0)$, $j = 1, \ldots, q-1$, holds; for $q \equiv 1 \pmod 4$

$$\begin{aligned} e_j(0) = 1 &+ \omega^{j\cdot 2} + \omega^{j\cdot 4} + \cdots + \omega^{j\cdot(q-1)/2} \\ &+ \omega^{j\cdot(q+1)/2} + \cdots + \omega^{j\cdot(q-4)} + \omega^{j\cdot(q-2)}; \end{aligned}$$

hence

$$\begin{aligned} -e_j(0) &= \omega^j + \omega^{j\cdot 3} + \omega^{j\cdot 5} + \cdots + \omega^{j\cdot(q-3)/2} \\ &\quad + \omega^{j\cdot(q+3)/2} + \cdots + \omega^{j\cdot(q-3)} + \omega^{j\cdot(q-1)} \\ &= \omega^j \cdot (1 + \omega^{j\cdot 2} + \omega^{j\cdot 4} + \cdots + \omega^{j\cdot(q-5)/2} \\ &\quad + \omega^{j\cdot(q+1)/2} + \cdots + \omega^{j\cdot(q-4)} + \omega^{j\cdot(q-2)}) \\ &= \omega^j \cdot (e_j(0) - \omega^{j\cdot(q-1)/2}), \end{aligned}$$

and so $e_j(0) = \omega^{j\cdot(q-1)/2}/(1+\omega^j) \neq 0$.

Analogously it can be shown that for $q \equiv -1 \pmod 4$, $e_j(0) = \omega^{j\cdot(q+1)/2}/(1+\omega^j) \neq 0$. So by (3.6) all the eigenvalues of $R^{n,0}$ and $R^{n,1}$ are different from 0, so that both matrices have full rank q^n. Applying the bounds (1.1) and (1.4) then yields $C_2(r_n) = \lceil n \cdot \log_2(q) \rceil + 1$.

4. HAMMING DISTANCE

For the function-value matrices $H^{n,k}$ of the Hamming distance the results of Section 2 are well known (see Delsarte, 1973, or Bannai and Ito, 1984), because those matrices form the Hamming association scheme. The eigenvalues $e_{i^n}(k)$ only depend on the weight $i := w(i^n)$ of $i^n \in \{0, \ldots, q-1\}^n$ and they are known as the Krawtchouk polynomials, so by (1.11), $e_{i^n}(k) = e_i(k, n) = K_k(i, n)$ with

$$K_k(i,n) = \sum_{j=0}^{k} \binom{i}{j} \cdot \binom{n-i}{k-j} \cdot (-1)^j \cdot (q-1)^{k-j} \quad \text{for } i, k = 0, \ldots, n,\ n \in \mathbb{N}. \tag{4.1}$$

In the book of MacWilliams and Sloane (1977, pp. 151–153) the following relations for the Krawtchouk polynomials can be found:

$$K_k(i,n) = \sum_{j=0}^{k} (-q)^j \cdot (q-1)^{k-j} \binom{n-j}{k-j} \cdot \binom{i}{j}, \tag{4.2}$$

$$\sum_{k=0}^{n} K_k(i,n) = \begin{cases} q^n, & i = 0 \\ 0, & i = 1, \ldots, n, \end{cases} \tag{4.3}$$

$$\sum_{k=0}^{n} K_k(i,n) \cdot z^k = (1 + (q-1)\cdot z^{n-i}) \cdot (1-z)^i. \tag{4.4}$$

From (4.4) the following recursion formulae can easily be derived:

$$K_k(i,n) = K_k(i-1, n-1) - K_{k-1}(i-1, n-1) \quad \text{for } i = 1, \ldots, n, \tag{4.5}$$

$$K_k(i,n) = K_k(i, n-1) + (q-1)\cdot K_{k-1}(i, n-1) \quad \text{for } i = 0, \ldots, n-1. \tag{4.6}$$

THEOREM 4.1. *Let $q := p_1^{e_1} \cdot \cdots \cdot p_r^{e_r}$ be the prime factorization of q, and let $n := p_s^m - 1$ for a prime factor p_s, $1 \leq s \leq r$, $m \in \mathbb{N}$. Then*

$$|C_2(h_n) - \lceil \log_2(n+1) \rceil - \lceil n \cdot \log_2(q) \rceil| \leq 1.$$

Proof. From (4.2) it follows that $K_k(i) \equiv (-1)^k \binom{p_s^m - 1}{k} \pmod{p_s}$ for $i, k = 0, \ldots, p_s^m - 1$. Now $p_s^m - 1 = (p_s - 1)\cdot p_s^{m-1} + (p_s-1)\cdot p_s^{m-2} + \cdots + (p_s-1)\cdot p_s + (p_s - 1)$, and for $k = k_{m-1}\cdot p_s^{m-1} + k_{m-2}\cdot p_s^{m-2} + \cdots + k_1 \cdot p_s + k_0$ ($k_j \in \{0, \ldots, p_s - 1\}$) a theorem of Lucas (see, e.g., Dickson, 1919, p. 271) can be applied to show that

$$\begin{aligned} \binom{p_s^m - 1}{k} &\equiv \binom{p_s - 1}{k_{m-1}} \cdot \binom{p_s - 1}{k_{m-2}} \cdot \cdots \\ &\quad \cdot \binom{p_s - 1}{k_1} \cdot \binom{p_s - 1}{k_0} \pmod{p_s} \\ &\neq 0 \pmod{p_s}, \text{ since } p_s - 1 \geq k_j \text{ for } j = 0, \ldots, m-1. \end{aligned}$$

Hence for $n = p_s^m - 1$, where p_s is a prime factor of q, all the eigenvalues of the matrices $H^{n,k}$ are different from 0, so that each of the matrices $H^{n,k}$, $k \in \{0, \ldots, n\}$, has full rank q^n. From the lower bound (1.4) it follows:

$$\begin{aligned} C_2(h_n) &\geq \lceil \log_2((n+1)\cdot q^n) \rceil = \lceil \log_2(n+1) + n \cdot \log_2(q) \rceil \\ &\geq \lceil \log_2(n+1) \rceil + \lceil n \cdot \log_2(q) \rceil - 1. \end{aligned}$$

Together with the upper bound (1.1) this yields

$$|C_2(h_n) - \lceil \log_2(n+1) \rceil - \lceil n \cdot \log_2(q) \rceil| \leq 1. \quad ∎$$

5. HAMMING DISTANCE (MODULO 3)

The function-value matrices of the function $d_n := h_n \pmod 3$ are

$$D^{n,j} = \sum_{t=0}^{\lfloor n/3 \rfloor} H^{n,3\cdot t+j}, \qquad j = 0, 1, 2. \tag{5.1}$$

Since the matrices $H^{n,k}$ are simultaneously diagonalized, the eigenvalues $e_i(j, n)$ of $D^{n,j}$ are linear combinations of the Krawtchouk polynomials, namely,

$$e_i(j, n) = \sum_{t=0}^{\lfloor n/3 \rfloor} K_{3\cdot t+j}(i, n), \quad i \in \{0, \ldots, n\},\ j \in \{0, 1, 2\}. \tag{5.2}$$

The recursion formulae (4.5) and (4.6) are inherited by the eigenvalues $e_i(j, n)$:

$$e_i(j, n) = e_{i-1}(j, n-1) - e_{i-1}(j-1 \pmod 3, n-1) \quad \text{for } i = 1, \ldots, n, \tag{5.3}$$

$$e_i(j, n) = e_i(j, n-1) + (q-1)\cdot e_i(j-1 \pmod 3, n-1) \quad \text{for } i = 0, \ldots, n-1, \tag{5.4}$$

with starting values $e_i(0, 1) = 1$ for $i = 0, 1$; $e_0(1, 1) = q-1$; $e_1(1, 1) = -1$, and $e_i(2, 1) = 0$ for $i = 0, 1$.

LEMMA 5.1.

$$e_i(j, n) = (-3)\cdot e_{i-2}(j-1 \pmod 3, n-2) \quad \textit{for } i, n \geq 3. \tag{5.5}$$

Proof. From (4.3) and (5.2) it follows that for $i, n \geq 1$,

$$e_i(0, n) + e_i(1, n) + e_i(2, n) = 0. \tag{5.6}$$

Applying twice the recursion formula (5.3) yields

$$\begin{aligned} e_i(j, n) &= e_{i-1}(j, n-1) - e_{i-1}(j-1 \pmod 3, n-1) \\ &= e_{i-2}(j, n-2) - 2\cdot e_{i-2}(j-1 \pmod 3, n-2) \\ &\quad + e_{i-2}(j-2 \pmod 3, n-2) \\ &= e_{i-2}(j, n-2) + e_{i-2}(j-1 \pmod 3, n-2) \\ &\quad + e_{i-2}(j-2 \pmod 3, n-2) \\ &\quad - 3\cdot e_{i-2}(j-1 \pmod 3, n-2) \\ &= (-3)\cdot e_{i-2}(j-1 \pmod 3, n-2)) \quad \text{by (5.6).} \end{aligned}$$

∎

For determining the communication complexity of d_n it is important to know, when the eigenvalues $e_i(j, n)$ are different from 0. From (5.5) it is clear that $e_i(j, n) \neq 0$, iff $e_{i-2}(j-1 \pmod 3, n-2) \neq 0$. So for arbitrary n we only have to examine the eigenvalues $e_i(j, n)$ for $i = 0, 1, 2$.

LEMMA 5.2. *Let $n \geq 2$, $q \geq 4$ and $i, j \in \{0, 1, 2\}$. Then*

$$e_i(j, n) \neq 0. \tag{5.7}$$

Proof. Case $i = 0$. (4.6) implies that

$$\begin{aligned} e_0(j, n) &= \sum_{t=0}^{\lfloor n/3 \rfloor} K_{3\cdot t+j}(0, n) \\ &= \sum_{t=0}^{\lfloor n/3 \rfloor} \binom{n}{3\cdot t+j}\cdot(q-1)^{3\cdot t+j} > 0 \\ &\qquad \text{for } n \geq 2,\ j \in \{0, 1, 2\}. \end{aligned}$$

Case $i = 1, 2$. Applying the recursion formula (5.3) we have for $n \geq 1$

$$\begin{aligned} e_1(0, n) &= e_0(0, n-1) - e_0(2, n-1) \\ &= \sum_{t=0}^{\lfloor (n-1)/3 \rfloor} K_{3\cdot t}(0, n-1) \\ &\quad - \sum_{t=0}^{\lfloor (n-1)/3 \rfloor} K_{3\cdot t+2}(0, n-1) \\ &= \sum_{t=0}^{\lfloor (n-1)/3 \rfloor} \binom{n-1}{3\cdot t}\cdot(q-1)^{3\cdot t} \\ &\quad - \sum_{t=0}^{\lfloor (n-1)/3 \rfloor} \binom{n-1}{3\cdot t+2}\cdot(q-1)^{3\cdot t+2} \\ &= 1 + \sum_{t=1}^{\lfloor (n-1)/3 \rfloor} \binom{n-1}{3\cdot t}\cdot(q-1)^{3\cdot t} \\ &\quad - \sum_{t=0}^{\lfloor (n-1)/3 \rfloor} \binom{n-1}{3\cdot t+2}\cdot(q-1)^{3\cdot t+2} \\ &\equiv 1 \pmod{q-1}, \end{aligned}$$

$$\begin{aligned} e_1(1, n) &= \sum_{t=0}^{\lfloor (n-1)/3 \rfloor} \binom{n-1}{3\cdot t+1}\cdot(q-1)^{3\cdot t+1} - 1 \\ &\quad - \sum_{t=1}^{\lfloor (n-1)/3 \rfloor} \binom{n-1}{3\cdot t}\cdot(q-1)^{3\cdot t} \equiv -1 \pmod{q-1}, \end{aligned}$$

$$\begin{aligned} e_1(2, n) &= \sum_{t=0}^{\lfloor (n-1)/3 \rfloor} \binom{n-1}{3\cdot t+2}\cdot(q-1)^{3\cdot t+2} \\ &\quad - \sum_{t=0}^{\lfloor (n-1)/3 \rfloor} \binom{n-1}{3\cdot t+1}\cdot(q-1)^{3\cdot t+1} \\ &\equiv 0 \pmod{q-1}. \end{aligned}$$

Applying recursion (5.3) once more yields for $n \geq 2$,

$$e_2(0, n) = e_1(0, n-1) - e_1(2, n-1) \equiv 1 \pmod{q-1},$$

$$e_2(1, n) = e_1(1, n-1) - e_1(0, n-1) \equiv -2 \pmod{q-1},$$

$$e_2(2, n) = e_1(2, n-1) - e_1(1, n-1) \equiv 1 \pmod{q-1}.$$

So for $n \geq 2$ and $q \geq 4$, $e_1(0, n)$, $e_1(1, n)$, $e_2(0, n)$, $e_2(1, n)$, $e_2(2, n) \neq 0 \pmod{q-1}$ and thus are different from 0, such that only $e_1(2, n)$ remains to be examined.

The eigenvalues $e_1(j, n)$ can be obtained by applying recursion (5.4): $e_1(j, n) = e_1(j, n-1) + (q-1) \cdot e_1(j-1 \pmod 3, n-1)$ with $e_1(0, 2) = 1$, $e_1(1, 2) = q-2$, and $e_1(2, 2) = -(q-1)$.

Computation modulo $(q-1) \cdot (q-2) + 1$ yields

$$\begin{aligned} e_1(0, 3) &= 1 - (q-1)^2 = 1 - (q-1) \cdot (q-2) - (q-1) \\ &= -(q-1) \cdot (q-2) - 1 - (q-3) \\ &= -(q-3) \pmod{(q-1) \cdot (q-2) + 1} \\ &\equiv -(q-3) \cdot e_1(0, 2) \pmod{(q-1) \cdot (q-2) + 1}, \end{aligned}$$

$$\begin{aligned} e_1(1, 3) &= (q-2) + (q-1) \\ &= (q-1) \cdot (q-2) + 1 - (q-2) \cdot (q-3) \\ &\equiv -(q-3) \cdot (q-2) \pmod{(q-1) \cdot (q-2) + 1} \\ &\equiv -(q-3) \cdot e_1(1, 2) \pmod{(q-1) \cdot (q-2) + 1}, \end{aligned}$$

$$\begin{aligned} e_1(2, 3) &= -(q-1) + (q-1) \cdot (q-2) \\ &= (q-1) \cdot (q-3) = -(q-3) \cdot (-(q-1)) \\ &\equiv -(q-3) \cdot e_1(2, 2) \pmod{(q-1) \cdot (q-2) + 1}. \end{aligned}$$

Hence for $j = 0, 1, 2$ it is $e_1(j, 3) \equiv -(q-3) \cdot e_1(j, 2) \pmod{(q-1) \cdot (q-2) + 1}$ and so $e_1(j, n) \equiv (-(q-3))^{n-2} \cdot e_1(j, 2) \pmod{(q-1) \cdot (q-2) + 1}$ for $n \geq 2$.

But now $(q-1) \cdot (q-2) + 1 - q \cdot (q-3) = 3$. Using the Euclidean algorithm it is clear that $\gcd((q-1) \cdot (q-2) + 1, q-3) = 1$ or 3. It can easily be verified that $(q-1) \cdot (q-2) + 1 \equiv 1, 3, 4,$ or $7 \pmod 9$. Hence $(q-1) \cdot (q-2) + 1$ is not divisible by 9. So there must exist a divisor of $(q-1) \cdot (q-2) + 1$ that is not a divisor of $(q-3)$. As for $j = 0, 1, 2$ also $\gcd(e_1(j, 2), (q-1) \cdot (q-2) + 1) = 1$, $e_1(j, n)$ is not divisible by $(q-1) \cdot (q-2) + 1$ and thus cannot be 0. Particularly, $e_1(2, n) \neq 0$ for $n \geq 2$. ∎

THEOREM 5.1. *Let $q \geq 4$ and $n \geq 1$. For the eigenvalues $e_i(j, n)$ of the matrices $D^{n,j}$ $e_i(j, n) \neq 0$ for $i = 0, \ldots, n-1$ and $j = 0, 1, 2$:*

If n is even, then $e_n(j, n) \neq 0$ for $j = 0, 1, 2$.

If $n = 2t+1$, $t \geq 0$, is odd, then

$$e_n(j, n) \begin{cases} = 0 & \text{for } j = t+2 \pmod 3 \\ \neq 0 & \text{for } j = t, t+1 \pmod 3. \end{cases}$$

Proof. (a) Let $n = 2 \cdot t$, $t \geq 1$. Induction on t: If $t = 1$, then $n = 2$ and $e_2(j, n) \neq 0$ for $i, j \in \{0, 1, 2\}$ by (5.7).

Now assume that the claim holds for $t-1$. By Lemma 5.2, $e_i(j, n) \neq 0$ for $i, j = 0, 1, 2$. Using (5.5) and the induction hypothesis it can be shown for $i = 3, \ldots, 2 \cdot t$ that

$$e_i(j, 2 \cdot t) = (-3) \cdot e_{i-2}(j-1 \pmod 3, 2 \cdot t - 2) \neq 0$$

$$\text{for } j = 0, 1, 2.$$

(b) Now let $n = 2 \cdot t + 1$, $t \geq 0$. Induction on t yields $e_1(0, 1) = 1$, $e_1(1, 1) = -1$, and $e_1(2, 1) = 0$.

Assume that the claim is proved for $t-1$. (5.7) implies that $e_i(2 \cdot t + 1) \neq 0$ for $i, j = 0, 1, 2$. For $i = 3, \ldots, 2 \cdot t + 1$, applying (5.5) and the induction hypothesis yields $e_i(j, 2 \cdot t + 1) = (-3) \cdot e_{i-2}(j-1 \pmod 3, 2 \cdot t - 1)$

$$\begin{cases} \neq 0 & \text{for } i = 3, \ldots, 2 \cdot t, \quad j = 0, 1, 2, \\ \neq 0 & \text{for } i = 2 \cdot t + 1, \quad j = t, t+1 \pmod 3, \\ = 0 & \text{for } i = 2 \cdot t + 1, \quad j = t+2 \pmod 3. \end{cases}$$ ∎

COROLLARY 5.1. *Let $q \geq 4$, $n \geq 2$. For the communication complexity of the function $d_n = h_n \pmod 3$ we have the following lower bounds:*

(a) $C_2(d_n) \geq \lceil n \cdot \log_2(q) + \log_2(3) \rceil$, *if n is even,*

(b) $C_2(d_n) \geq \lceil \log_2(3 \cdot q^n - (q-1)^n) \rceil$, *if n is odd.*

Proof. If n is even, then by Theorem 5.1 all the eigenvalues of the function-value matrices $D^{n,j}$, $j = 0, 1, 2$, are different from 0. Thus these matrices have full rank q^n, so that the lower bound (1.4) yields $C_2(d_n) \geq \lceil \log_2(3 \cdot q^n) \rceil = \lceil \log_2(3) + n \cdot \log_2(q) \rceil$.

(b) If $n = 2 \cdot t + 1$ is odd, then by Theorem 5.1, $e_n(t+2 \pmod 3, n) = 0$, whereas all the other eigenvalues of the function-value matrices are different from 0. In $\{0, \ldots, q-1\}^n$ there are $(q-1)^n$ elements with Hamming weight n, so that the eigenvalue $e_n(t+2 \pmod 3, n)$ has multiplicity $(q-1)^n$. Thus $D^{n, t+2 \pmod 3}$ has rank $q^n - (q-1)^n$, whereas $D^{n, t \pmod 3}$ and $D^{n, t+1 \pmod 3}$ have full rank q^n. So the lower bound (1.4) yields $C_2(d_{2 \cdot t+1}) \geq \lceil \log_2(3 \cdot q^{2 \cdot t+1} - (q-1)^{2 \cdot t+1}) \rceil$. ∎

6. LEE DISTANCE

For $x^n := (x_1, \ldots, x_n)$, $y^n := (y_1, \ldots, y_n) \in X^n$, $X := \{0, \ldots, q-1\}$, the Lee distance $l_n(x^n, y^n) = \sum_{i=1}^n l(x_i, y_i)$ is defined by $l(x, y) := \min\{|x-y|, q - |x-y|\}$. (2.6) gives the representation for the matrices $L^{1,k}$, $k := 0, \ldots, \lfloor q/2 \rfloor$: $L^{1,0} = Z_q^0 = I$, $L^{1,k} = Z_q^k + Z_q^{q-k}$ for $k := 1, \ldots, \lceil q/2 \rceil - 1$, and $L^{1, q/2} = Z_q^{q/2}$, if q is even.

By (2.11) the eigenvalues $e_j(k)$ of the matrices $L^{1,k}$ (again ω is a qth root of unity) are $e_j(0) = 1$ for $j := 0, \ldots, q-1$; $e_j(q/2) = \omega^{j \cdot q/2} = (-1)^j$ for $j := 0, \ldots, q-1$, if q is even;

and $e_j(k) = e_{q-j}(k) = \omega^{jk} + \omega^{j(q-k)} = 2 \cdot \cos(2\pi \cdot j \cdot k/q)$ for $j := 0, ..., q-1$, $k := 1, ..., \lceil q/2 \rceil - 1$. Hence with $i^n := (i_1, ..., i_n) \in \{0, ..., q-1\}^n$ (2.13) yields the following generating function for the eigenvalues $e_{i^n}(k)$, $k := 0, ..., \lfloor q/2 \rfloor \cdot n$:

$$\sum_{k=0}^{\lfloor q/2 \rfloor \cdot n} e_{(i_1, ..., i_n)}(k) \cdot z^k = \begin{cases} \prod_{j=1}^{n} \left(1 + 2\cos\left(\frac{2\pi i_j}{q}\right) \cdot z + 2\cos\left(\frac{4\pi i_j}{q}\right) \cdot z^2 + \cdots \right. \\ \qquad \left. + 2\cos\left(\frac{(q-1)\,\pi i_j}{q}\right) \cdot z^{(q-1)/2}\right), \qquad q \text{ odd} \\ \prod_{j=1}^{n} \left(1 + 2\cos\left(\frac{2\pi i_j}{q}\right) \cdot z + \cdots + 2\cos\left(\frac{(q-2)\,\pi i_j}{q}\right) \right. \\ \qquad \left. \cdot z^{(q-2)/2} + (-1)^{i_j} \cdot z^{q/2}\right), \qquad q \text{ even.} \end{cases} \tag{6.1}$$

(The same formula is obtained by replacing the variables z_i by z^i $(i = 1, ..., \lfloor q/2 \rfloor)$ in the generating function for the eigenvalues of the Lee association scheme (see Astola, 1982, or Sole, 1989).

This formula seems to be too complicated to examine which eigenvalues are different from 0. But from (2.11) it is known that every eigenvalue $e_{i^n}(k)$ can be represented as a sum of the roots of unity. Hence,

$$e_{i^n}(k) = a_0 + a_1 \cdot \omega + a_2 \cdot \omega^2 + \cdots + a_{q-1} \cdot \omega^{q-1} \quad \text{for some } a_0, ..., a_{q-1} \in \mathbb{N}. \tag{6.2}$$

If the alphabet size q is a prime number, then $\{1, \omega, ..., \omega^{q-2}\}$ is a basis of the integers in the field $\mathbb{Q}(\omega)$. Particularly the representation $0 = 1 + \omega + \omega^2 + \cdots + \omega^{q-1}$ is unique up to scalar multiplication.

So $e_{i^n}(k) = 0$ can only occur if $a_0 = a_1 = \cdots = a_{q-1}$. But then $e_{i^n}(k)$ is a sum of A roots of unity, where A is a number divisible by q. From (2.11) we know that A is the number of elements $t^n \in X^n$ with Lee weight $w(t^n) = k$, so A only depends on n and k and not on the special choice of i^n. Thus,

$$A = \sum_{\substack{t^n \in X^n: \\ w(t^n) = k}} 1 = \sum_{\substack{t^n \in X^n: \\ w(t^n) = k}} \omega^0 = e_{(0, ..., 0)}(k) =: a(n, k).$$

From (6.1) we obtain the generating function

$$\sum_{k=0}^{\lfloor (q-1)/2 \rfloor \cdot n} a(n, k) \cdot z^k = (1 + 2z + 2z^2 + \cdots + 2z^{\lfloor (q-1)/2 \rfloor})^n. \tag{6.3}$$

So the following recursion holds:

$$\begin{aligned} a(n, k) &= a(n-1, k) + 2 \cdot a(n-1, k-1) \\ &\quad + 2 \cdot a(n-1, k-2) + \cdots \\ &\quad + 2 \cdot a\left(n-1, k - \frac{q-1}{2}\right) \\ &\quad \text{with} \quad a(1, 0) = 1, \quad a(1, j) = 2 \\ &\quad \text{for} \quad j := 1, ..., \frac{q-1}{2}. \end{aligned} \tag{6.4}$$

Now let $\Theta := (q-1)/2$ and let $\binom{n}{k_0 \cdots k_\Theta}$ be the multinomial coefficient. Now $(z_0 + z_1 + \cdots + z_\Theta)^n = \sum_{k_0 + \cdots + k_\Theta = n} \binom{n}{k_0 \cdots k_\Theta} \cdot z_0^{k_0} \cdot z_1^{k_1} \cdot \cdots \cdot z_\Theta^{k_\Theta}$; hence with $z_0 := 1$, $z_1 := 2z$, $z_2 := 2z^2$, ..., $z_\Theta := 2z^\Theta$,

$$a(n, k) = \sum_{\substack{k_0 + k_1 + \cdots + k_\Theta = n \\ k_1 + 2k_2 + \cdots + \Theta k_\Theta = k}} \binom{n}{k_0 \cdots k_\Theta} \cdot 2^{n - k_0}. \tag{6.5}$$

LEMMA 6.1. *Let q be a prime number, and let $n = q^s + 2 \cdot q^{s-1} + \cdots + 2 \cdot q + 2$ or $n = 2 \cdot q^s + 2 \cdot q^{s-1} + \cdots + 2 \cdot q + 2$, $s \in \mathbb{N}$. Then the number $a(n, k)$ of elements $t^n \in \{0, ..., q-1\}^n$ with Lee weight $w(t^n) = k$ is not divisible by q.*

Proof. Let the q-adic representation of the numbers n, k, k_0, ..., k_Θ $(\Theta := (q-1)/2)$ be $n = a_s q^s + a_{s-1} q^{s-1} + \cdots + a_1 q + a_0$, $k = b_s q^s + b_{s-1} q^{s-1} + \cdots + b_1 q + b_0$, $k_i = b_{is} q^s + \cdots + b_{i1} q + b_{i0}$, with $a_j, b_j, b_{ij} \in \{0, ..., q-1\}$. Now (see, e.g., Dickson, 1919, p. 273)

$$\binom{n}{k_0 \cdots k_\Theta} \equiv \binom{a_s}{b_{0s} \cdots b_{\Theta s}} \cdot \cdots \cdot \binom{a_1}{b_{01} \cdots b_{\Theta 1}} \cdot \binom{a_0}{b_{00} \cdots b_{\Theta 0}} \pmod q. \tag{6.6}$$

(6.3) and (6.4) yield for $n = 2q^s + 2q^{s-1} + \cdots + 2q + 2$, $s \in \mathbb{N}$:

$$\begin{aligned} a(n, k) &= \sum_{\substack{k_0 + k_1 + \cdots + k_\Theta = n \\ k_1 + 2k_2 + \cdots + \Theta k_\Theta = k}} \binom{n}{k_0 \cdots k_\Theta} \cdot 2^{n - k_0} \\ &\equiv \sum_{\substack{k_0 + k_1 + \cdots + k_\Theta = n \\ k_1 + 2k_2 + \cdots + \Theta k_\Theta = k}} \binom{2}{b_{0s} \cdots b_{\Theta s}} \cdot \cdots \\ &\quad \cdot \binom{2}{b_{00} \cdots b_{\Theta 0}} \cdot 2^{n - k_0} \pmod q \\ &\equiv \sum_{\substack{b_{0s} q^s + \cdots + b_{00} + \cdots + b_{\Theta s} q^s + \cdots + b_{\Theta 0} = 2q^s + \cdots + 2 \\ b_{1s} q^s + \cdots + b_{10} + \cdots + \Theta b_{\Theta s} q^s + \cdots + \Theta b_{\Theta 0} = b_{1s} q^s + \cdots + b_{\Theta 0}}} \\ &\quad \times \binom{2}{b_{0s} \cdots b_{\Theta s}} \cdots \binom{2}{b_{00} \cdots b_{\Theta 0}} 2^{(2 - b_{0s}) q^s} \cdots 2^{2 - b_{00}} \pmod q. \end{aligned}$$

Since q is a prime number, $2^q \equiv 2 \pmod q$; and if $b_{0j} + \cdots + b_{\Theta j} > 2$ for some j, then the corresponding summand is con-

gruent 0 (mod q). So one only has to sum up those terms with $b_{0j}+\cdots+b_{\Theta j}\leqslant 2$. But then $b_j\leqslant 2\cdot\Theta=q-1<q$, so that

$$\begin{aligned}a(n,k)\equiv & \sum_{\substack{b_{00}q^0+\cdots+b_{\Theta 0}q^0=2q^0\\ b_{01}q^1+\cdots+\Theta b_{\Theta 1}q^1=b_1q^1}}\cdots\\ & \sum_{\substack{b_{0s}+\cdots+b_{\Theta s}=2\\ b_{1s}+\cdots+\Theta b_{\Theta s}=b_s}}\binom{2}{b_{0s}\cdots b_{\Theta s}}\\ & \cdot 2^{2-b_{0s}}\cdots\binom{2}{b_{00}\cdots b_{\Theta 0}}\cdot 2^{2-b_{00}}\pmod q\\ \equiv & \left(\sum_{\substack{b_{0s}+\cdots+b_{\Theta s}=s\\ b_{1s}+\cdots+\Theta b_{\Theta s}=b_s}}\binom{2}{b_{0s}\cdots b_{\Theta s}}\cdot 2^{2-b_{0s}}\right)\cdots\\ & \left(\sum_{\substack{b_{00}+\cdots+b_{\Theta 0}=2\\ b_{10}+\cdots+\Theta b_{\Theta 0}=b_0}}\binom{2}{b_{00}\cdots b_{\Theta s}}\cdot 2^{2-b_{00}}\right)\pmod q\\ \equiv & a(2,b_s)\cdot\cdots\cdot a(2,b_1)\cdot a(2,b_0)\pmod q\\ \neq & 0\pmod q,\end{aligned}$$

since (6.4) implies that $a(2,0)=1$, and for $k=1,\ldots,2\cdot\Theta=q-1$ $a(2,k)$ is an even number. Moreover, $a(2,k)\leqslant 2\cdot(q-1)$ and thus not divisible by q.

An analogous computation yields for $n=q^s+2q^{s-1}+\cdots+2q+2$, $s\in\mathbb{N}$, $a(n,k)\equiv a(1,b_s)\cdot a(2,b_{s-1})\cdot\cdots\cdot a(2,b_1)\cdot a(2,b_0)\pmod q\neq 0\pmod q$. ∎

COROLLARY 6.1. *Let the alphabet size q be a prime number. Then for $n=q^s+2q^{s-1}+\cdots+2q+2$ and $n=2q^s+2q^{s-1}+\cdots+2q+2$, $s\in\mathbb{N}$, the communication complexity $C_2(l_n)$ of the Lee distance is bounded by*

$$\left|C_2(l_n)-\lceil n\cdot\log_2(q)\rceil-\left\lceil\log_2\left(\frac{q-1}{2}\cdot n+1\right)\right\rceil\right|\leqslant 1.$$

Proof. From the preceding lemma we know that the number $a(n,k)$ of roots of unity in the sum $e_{i^n}(k)=a_0+a_1\omega+\cdots+a_{q-1}\omega^{q-1}$ is not divisible by q for every eigenvalue $e_{i^n}(k)$ of the matrices $L^{n,k}$. Hence all the eigenvalues must be different from 0, so that the lower bound (1.4) can be applied to obtain

$$\begin{aligned}C_2(l_n)&\geqslant\lceil\log_2(\operatorname{rank}(L^{n,0})+\cdots+\operatorname{rank}(L^{n,(q-1)/2})\rceil\\ &=\left\lceil\log_2\left(\left(\frac{q-1}{2}\cdot n+1\right)\cdot q^n\right)\right\rceil\\ &=\left\lceil n\cdot\log_2(q)+\log_2\left(\frac{q-1}{2}\cdot n+1\right)\right\rceil.\end{aligned}$$

Moreover, the upper bound (1.1) yields $C_2(l_n)\leqslant\lceil n\cdot\log_2(q)\rceil+\lceil\log_2(((q-1)/2)\cdot n+1)\rceil$, such that $|C_2(l_n)-\lceil n\cdot\log_2(q)\rceil-\lceil\log_2(((q-1)/2)\cdot n+1)\rceil|\leqslant 1$. ∎

Remark. With the same method of proof for the function $s_n: X^n\times X^n$ with $s_n((x_1,\ldots,x_n),(y_1,\ldots,y_n))=\sum_{i=1}^n[(y_i-x_i)\pmod q]$, it can be shown that $|C_2(s_n)-n\cdot\log_2(q)-\log_2((q-1)\cdot n+1)|\leqslant 1$ for $n=q^s+q^{s-1}+\cdots+q+1$, $s\in\mathbb{N}$, if q is a prime number.

Received February 28, 1991

ACKNOWLEDGMENT

I thank Professor R. Ahlswede for helpful discussions.

REFERENCES

Ahlswede, R. (1989), On code pairs with specified Hamming distances, *in* "Colloq. Math. Soc. János Bolyai," pp. 9–47, Vol. 52, North Holland, Amsterdam.

Ahlswede, R., Cai, N., and Zhang, Z. (1989), A general 4-words inequality with consequences for 2-way communication complexity, *Adv. in Appl. Math.* **10**, 75–94.

Ahlswede, R., and Mörs, M. (1988), Inequalities for code pairs, *Europ. J. Combin.* **9**, 175–188.

Astola, J. (1982), The theory of Lee codes, Lappeenranta research report, 1982 (unpublished).

Bannai, E., and Ito, T. (1984), "Algebraic Combinatorics I," Benjamin–Cummings, Menlo Park, CA.

Chihara, L., and Stanton, D. (1990), Zeros of generalized Krawtchouk polynomials, *J. Approx. Theory* **60**, 43–57.

Davis, P. J. (1979), "Circulant Matrices," Wiley, New York.

Delsarte, P. (1973), "An Algebraic Approach to the Association Schemes of Coding Theory," Philips Res. Rpts. Suppl., No. 10 (unpublished).

Diaconis, P., and Graham, R. L. (1985), The Radon transform on Z_2^k, *Pacific J. Math.* **118**, No. 2, 323–345.

Dickson, L. E. (1919), "Theory of Numbers," Vol. 1, Chelsea, New York, 1919.

El Gamal, A., and Pang, K. F. (1986), Communication complexity of computing the Hamming distance, *SIAM J. Comput.* **15**, No. 4, 932–947.

Halstenberg, B. (1986), "Zweiprozessor–Kommunikationskomplexität," Diplom thesis, Universität Bielefeld (unpublished).

Lovasz, L. (1990), Communication complexity: A survey, *in* "Paths, Flows and VLSI-Layout" (B. Korte, L. Lovasz, H. J. Prömel, and A. Schrijver, Eds.), pp. 235–266, Springer-Verlag, New York/Berlin.

Mehlhorn, K., and Schmidt, E. M. (1982), Las Vegas is better than determinism in VLSI and distributed computing, *in* "Proceedings, 14th Annual ACM Symposium on Theory of Computing, 1982," pp. 330–337.

MacWilliams, F. J., and Sloane, N. J. A. (1977), "The Theory of Error Correcting Codes," North Holland, Amsterdam.

Orlitsky, A., and El Gamal, A. (1988), Communication complexity, *in* "Complexity in Information Theory" (Y. Abu-Mostafa, Ed.), pp. 16–61, Springer-Verlag, New York/Berlin.

Sole, P. (1989), The Lee association scheme, INRIA Research Report (unpublished).

Spieker, B. (1992), Deterministic communication complexity of the Hamming distance, Memorandum No. 1026, Faculty of Applied Mathematics, University of Twente, Enschede (unpublished).

van Lint, J. H. (1975), A survey of perfect codes, *Rocky Mountain J. Math.* **5**, No. 2, 199–224.

Yao, A. (1979), Some complexity questions related to distributive computing, *in* "Proceedings, 11th Annual ACM Symp. Theory of Computing, 1979," pp. 209–219.